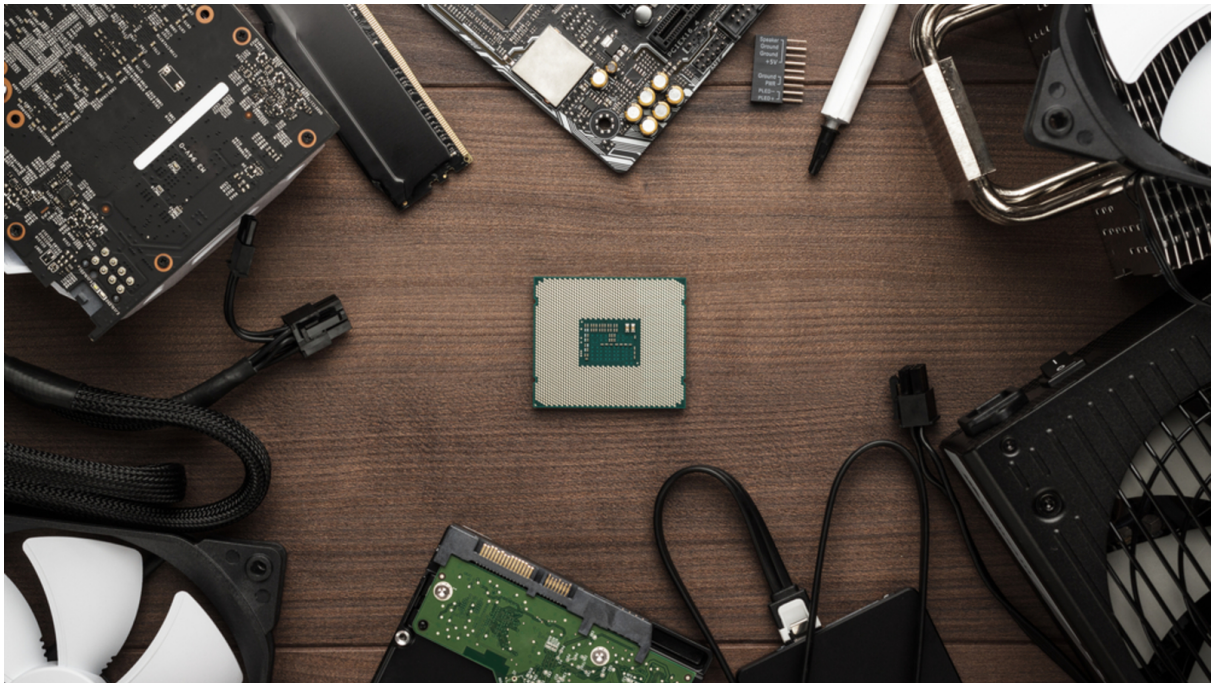

Freitag, 26. Januar 2018, 10:58 Uhr
~4 Minuten Lesezeit

Meltdown und Spectre

Waren es Verbrecher, die Dienste — oder wer?

von Wolfgang Romey
Foto: Ruslan Grumble/Shutterstock.com

In den letzten Tagen geistern wieder neue Begriffe durch die Medien: Meltdown und Spectre. Sie bezeichnen die bisher größte Sicherheitskatastrophe, die die Computerhersteller und -nutzer bislang

getroffen hat. Anders als meistens ist diesmal nicht die Software der Rechner betroffen, das kann durch neue Versionen behoben werden, sondern die Hardware. Seit etwa 20 Jahren sind die zentralen Bausteine von Computern, die CPUs, so aufgebaut, dass sie die mit Meltdown und Spectre bezeichneten Angriffsflächen bieten. Wie konnte es dazu kommen?

Gordon Moore äußerte 1965 in einem Artikel, dass sich die Leistungsfähigkeit von digitalen Schaltkreisen etwa alle 18 Monate verdoppeln würde, ohne dass die Kosten der Schaltkreise sich deutlich erhöhen. Das hat in den zurückliegenden Jahrzehnten zu einer Steigerung der Leistungsfähigkeit der Computer auf das 10 Milliardenfache geführt (1, 2).

Die Hersteller integrierter Schaltkreise sind seit langem in einem Konkurrenzkampf darum, wer die schnellsten Schaltkreise anbietet, denn der wird die höchsten Stückzahlen verkaufen. Da die Leistungssteigerung durch die Verbesserung im Herstellungsprozess nur noch mit sehr hohem Aufwand zu erreichen ist, ging man vor etwa 20 Jahren dazu über, Fortschritte durch die Weiterentwicklung der Architektur der CPUs zu erzielen, was zu einem immer komplexeren Aufbau geführt hat.

Die CPUs werden inzwischen durch umfangreiche, komplexe Programme gesteuert, die für die eigentliche Ausführung der Anwendersoftware sorgen. Diese Programme hätten intensiv auf Fehler und Angriffsmöglichkeiten geprüft werden müssen. Das ist teuer und könnte Auslieferungstermine verzögern, deshalb ist das nicht in ausreichender Tiefe erfolgt. Das fällt den Herstellern jetzt auf die Füße.

Ein weiterer Grund ist, dass auch aus Gründen der Konkurrenz der Programmtext der in der Hardware enthaltenen Programme nicht offengelegt wird. Hätte der Programmtext von Experten untersucht werden können, wären die Schwachstellen mit sehr großer Sicherheit schon sehr viel früher entdeckt worden.

Die vom Markt getriebene Konkurrenz der Hardwarehersteller ist also ein wesentlicher Grund für die Sicherheitskatastrophe. Unser Wirtschaftssystem zerstört nicht nur das Klima, sondern auch die Computersicherheit!

Waren es die Dienste?

Es gibt Stimmen, die davon ausgehen, dass die Hintertür nicht zufällig entstanden ist, sondern auf Vorgabe der „Dienste“ eingebaut wurde. Nach den Erfahrungen der letzten Jahre wäre das nicht überraschend. Da die Veränderung der Architektur der Hardware aber aus meiner Sicht wohl begründet und sinnvoll war, gehe ich nicht davon aus, dass die Sicherheitslücke schon vor mehr als 20 Jahren gezielt in die Architektur eingebaut wurde.

Man muss sich natürlich fragen, wann vom wem die Möglichkeit entdeckt wurde, die neue Architektur für Angriffe auszunutzen. Da für Dienste die Geheimhaltung des Programmtextes mit großer Sicherheit nicht gilt, kann man davon ausgehen, dass die Sicherheitslücke nicht erst vor kurzer Zeit aufgedeckt wurde. Vielleicht führt die Untersuchung vergangener Angriffe auf Rechner dazu, dass man den Zeitpunkt eingrenzen kann. Klar ist auch, dass Sicherheitslücken für alle nutzbar sind, also auch für Akteure mit verbrecherischen Absichten. Vielleicht haben sie die Sicherheitslücke schon früh gefunden.

Es ist allerdings merkwürdig, dass ausgerechnet Google, das doch

sehr gute Kontakte zu den Geheimdiensten hat, die Sicherheitslücke aufgedeckt hat. Vielleicht waren hier die wirtschaftlichen Interessen wichtiger als die staatlichen. Die gefundene Angriffsmöglichkeit beeinträchtigt nämlich massiv die Sicherheit des Cloud-Computings, also die Verlagerung von Daten und ihre Verarbeitung in riesige Rechenzentren, deren Sicherheit durch die Sicherheitslücke massiv auch bei den IT-Schwergewichten wie Amazon, Microsoft Facebook und Google gefährdet ist.

Vielleicht waren aber auch Forscher bei ihren Untersuchungen so weit fortgeschritten, dass die Aufdeckung des Fehlers durch die Wissenschaft drohte.

Bemerkenswert ist auch ein weiterer Aspekt. Die Entwickler des freien Betriebssystems Linux sind erst sehr spät informiert worden, obwohl Linux die meisten Rechner der Clouds antreibt. Es besteht also noch einiger Klärungsbedarf. Ich bin gespannt.

Was tun? Wenn man sich als normaler Nutzer weiterhin sicherheitsbewusst verhält, ist das vorhandene Risiko aus meiner Sicht nicht wesentlich größer geworden. Also weiterhin keine Dateien aus unbekannten Quellen herunterladen, keine E-Mails mit unbekanntem Absender oder deren Anhänge öffnen, den Internet-Browser mit Add-Ons ausstatten, die die Sicherheit erhöhen, Vorsicht beim Surfen, starke Passwörter wählen und sie regelmäßig ändern.

Also für den normalen Nutzer „Alles nicht so schlimm“? Doch! Denn hier wird deutlich, wie weit die Nutzer von wenigen US-Amerikanischen Hardwareherstellern abhängen. Ein Wechsel ist praktisch nicht möglich.

Quellen und Anmerkungen:

(1) **https://de.wikipedia.org/wiki/Mooresches_Gesetz** (https://de.wikipedia.org/wiki/Mooresches_Gesetz)
(2) **https://freedom-to-tinker.com/2018/01/04/singularity-skepticism-2-why-self-improvement-isnt-enough/** (https://freedom-to-tinker.com/2018/01/04/singularity-skepticism-2-why-self-improvement-isnt-enough/)

Dieser Artikel erschien bereits auf www.rubikon.news.

Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.

Dieses Werk ist unter einer **Creative Commons-Lizenz** (**Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de)) lizenziert. Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.